APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/605,689	10/17/2003	James M. Doherty	1033-T00534C	2688

60533   7590   02/05/2008

TOLER LAW GROUP
8500 BLUFFSTONE COVE
SUITE A201
AUSTIN, TX 78759

EXAMINER
GERGISO, TECHANE

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
02/05/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
	10/605,689	DOHERTY ET AL.
Office Action Summary	Examiner	Art Unit
	Techane J. Gergiso $\langle T - G$	2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>19 October 2007</u>.

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-24* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-24* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____ .

DETAILED ACTION

1.   In view of the Pre-Appeal filed on October 19, 2007, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

Claim Rejections - 35 USC § 103

2.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3.   Claims 1, 10 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Moran (US Pat. No.: 6, 647, 400) in view of Douglas (US Pub. No.: 2004/0049693).

As per claim 1:

Moran discloses an method for detecting intrusion in a host via a monitoring daemon

operating in conjunction with a configuration file defining data entities to be monitored, the

method comprising:

monitoring data entities via comparing a locally stored copy of a digital signature

associated with each data entity against a corresponding digital signature stored in a first

remote database (column 4: lines 1-15; figure 9: compute signature of a file; Does signature

match the previously computed signature for file; Abstract; column 4: lines 17-23; column

32: lines 49-59).

Moran does not explicitly disclose upon identifying a mismatch in compared digital

signatures, issuing an instruction to record an entry in a log file located in a second remote

database, said entry identifying a possible intrusion in a host. Douglas, in analogous art,

however, discloses upon identifying a mismatch in compared digital signatures, issuing an

instruction to record an entry in a log file located in a second remote database, said entry

identifying a possible intrusion in a host (0046; centralized log file; 0067; log server; syslog;

0111; 0155; 0177). Therefore, it would have been obvious to a person having ordinary skill in

the art at the time the invention was made to modify the system disclosed by Moran to include

upon identifying a mismatch in compared digital signatures, issuing an instruction to record an

entry in a log file located in a second remote database, said entry identifying a possible intrusion

in a host. This modification would have been obvious because a person having ordinary skill in

the art would have been motivated to do so to provide an efficiently managing and reporting

intrusion, or attempted intrusion, events of a computer network as suggested by Douglas (0004).

As per claim 10:

Moran discloses a system to detect intrusion comprising:

a host running a monitoring daemon working in conjunction with a configuration file,

said configuration file identifying files and directories to be monitored in said host and said

host communicating with external networks via one or more network interfaces, said

monitoring daemon dynamically monitoring said files and directories identified by said

configuration file by comparing a locally stored digital signature corresponding to each file

or directory against a remotely stored corresponding digital signature (column 4: lines 1-15;

figure 9: compute signature of a file; Does signature match the previously computed

signature for file);

a digital signature database remote from said host storing said digital signatures

associated with files and directories identified by said configuration file (Abstract; column 4:

lines 17-23; column 32: lines 49-59); and

a log database remote from said host recording entries corresponding to mismatches

between a digital signature stored in said host and a corresponding digital signature in said

digital signature database (column 32: lines 6-22; column 32: lines 49-59; column 33: lines

36-41).

Moran does not explicitly disclose a log database remote from said host recording entries

corresponding to mismatches between a digital signature stored in said host and a corresponding

digital signature in said digital signature database. Douglas, in analogous art, however, discloses

a log database remote from said host recording entries corresponding to mismatches between a

digital signature stored in said host and a corresponding digital signature in said digital signature

database (0046; centralized log file; 0067; log server; syslog; 0111; 0155; 0177). Therefore, it

would have been obvious to a person having ordinary skill in the art at the time the invention was

made to modify the system disclosed by Moran to include a log database remote from said host

recording entries corresponding to mismatches between a digital signature stored in said host and

a corresponding digital signature in said digital signature database. This modification would have

been obvious because a person having ordinary skill in the art would have been motivated to do

so to provide an efficiently managing and reporting intrusion, or attempted intrusion, events of a

computer network as suggested by Douglas (0004).

As per claim 15:

Moran discloses an article of manufacture comprising a computer usable medium having

computer readable program code embedded therein to detect intrusion in a host via a monitoring

daemon operating in conjunction with a configuration file defining data entities to be monitored,

said medium comprising:

computer readable program code comprising executable instructions to monitor data entities via comparing a locally stored copy of a digital signature associated with each data entity against a corresponding digital signature stored in a first remote database (column 4: lines 1-15; figure 9: compute signature of a file; Does signature match the previously computed signature for file; Abstract; column 4: lines 17-23; column 32: lines 49-59);

Moran does not explicitly disclose computer readable program code comprising executable instructions to issue an instruction to record an entry in a log file located in a second remote database upon identifying a mismatch in compared digital signature, said entry identifying a possible intrusion in said host. Douglas, in analogous art, however, discloses computer readable program code comprising executable instructions to issue an instruction to record an entry in a log file located in a second remote database upon identifying a mismatch in compared digital signature, said entry identifying a possible intrusion in said host (0046; centralized log file; 0067; log server; syslog; 0111; 0155; 0177). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Moran to include computer readable program code comprising executable instructions to issue an instruction to record an entry in a log file located in a second remote database upon identifying a mismatch in compared digital signature, said entry identifying a possible intrusion in said host. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide an efficiently managing and reporting intrusion, or attempted intrusion, events of a computer network as suggested by Douglas (0004).

4.   Claims 2-9, 11-14, 16-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Moran (US Pat. No.: 6, 647, 400) in view of Douglas (US Pub. No.: 2004/0049693) and further

in view of Trostle (US Pat. No.: 5, 919, 257).

As per claim 2:

Moran and Douglas do not explicitly disclose issuing a command to bring down said one

or more network interfaces to isolate and host upon identifying the mismatch in compared digital

signatures. Trostle, in analogous art, however, discloses issuing a command to bring down said

one or more network interfaces to isolate and host upon identifying the mismatch in compared

digital signatures (figure 4: 78-96; figure 5: 100; column 6: lines 30-42). Therefore, it would

have been obvious to a person having ordinary skill in the art at the time the invention was made

to modify the system disclosed by Moran and Douglas to include issuing a command to bring

down said one or more network interfaces to isolate and host upon identifying the mismatch in

compared digital signatures. This modification would have been obvious because a person

having ordinary skill in the art would have been motivated to do so to provide a trusted technique

for detecting illicit changes to executable programs (e.g., a "Trojan horse" appended to an

executable program by a computer hacker) as suggested by Trostle in (column 3: lines 19-28).

As per claim 3:

Trostle discloses issuing a command to an operating system of the host to bring said host to a single user state upon identifying the mismatch in compared digital signatures (figure 4: 78-96; figure 5: 100; column 6: lines 30-42).

As per claim 4:

Trostle discloses said first remote database and said second remote database are located on a single server or a plurality of servers belonging to a local area network (column 3: lines; 54-65figure 1: 12).

As per claim 5:

Trostle discloses communications between said host and first remote database are encrypted (column 5: lines 50-63; figure 5: 88).

As per claim 6:

Trostle discloses communications between said host and second remote database are encrypted (column 5: lines 50-63; figure 5: 88).

As per claim 7:

Moran discloses said digital signature is an MD5 signature and said first remote database is an MD5 database (column 31: lines 46-55).

As per claim 8:

Moran discloses said second remote database is a SYSLOG database (column 24: lines 47-64).

As per claim 9:

Moran discloses said data entities comprises one or more system files, configuration files, or directories (column 4: lines 5-35).

As per claim 11:

Moran discloses a system to detect intrusion, wherein said digital signature database and said log database are located on a single server or a plurality of servers belonging to a local area network (figure 3: 306, 308, 304).

As per claim 12:

Trostle discloses a system to detect intrusion, wherein communications between said host and said digital signature database are encrypted (column 5: lines 50-63; figure 5: 88).

As per claim 13:

Trostle discloses a system to detect intrusion, wherein communications between said host and log database are encrypted (column 5: lines 50-63; figure 5: 88).

As per claim 14:

Moran discloses a system to detect intrusion, wherein said digital signature is an MD5 signature and said first remote database is an MD5 database (column 31: lines 46-55).

As per claim 16:

Trostle discloses an article of manufacture, further comprising computer readable program code comprising executable instructions to issue a command to bring down one or more network interfaces to isolate said host upon identifying the mismatch in compared digital signatures (figure 4: 78-96; figure 5: 100; column 6: lines 30-42).

As per claim 17:

Trostle discloses an article of manufacture, the step of issue a command to an operating system of said host to bring said host to a single user state upon identifying the mismatch in compared digital signatures (figure 4: 78-96; figure 5: 100; column 6: lines 30-42).

As per claim 18:

Moran discloses an intrusion detection and isolation method implemented using a monitoring daemon in a host, said host having one or more network interfaces to communicate over one or more networks, said method comprising:

reading a configuration file to identify data entities to be monitored on a host (column 4: lines 1-15);

for each data entity to be monitored, extracting a digital signature from said host (figure 9: compute signature of a file);

for each data entity to be monitored, querying a remote digital signature database via said one or more network interfaces and requesting a digital signature corresponding to said digital signature extracted from said host (figure 9: Does signature match the previously computed signature for file);

for each data entity to be monitored, receiving said corresponding digital signature from said remote digital signature database (figure 3: 308, 306, 304, 312); and

matching digital signature received from said remote digital signature database with digital signature extracted at said host (Abstract; column 4: lines 17-23; column 32: lines 49-59).

Moran does not explicitly disclose upon identifying a mismatch, transmitting an instruction to a remote log database via said one or more network interfaces, said instruction executed in said remote log database to record an entry in a log file indicating a possible intrusion in said host. Douglas, in analogous art, however, discloses upon identifying a mismatch, transmitting an instruction to a remote log database via said one or more network interfaces, said instruction executed in said remote log database to record an entry in a log file indicating a possible intrusion in said host (0046; centralized log file; 0067; log server; syslog;

0111; 0155; 0177). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Moran to include upon identifying a mismatch, transmitting an instruction to a remote log database via said one or more network interfaces, said instruction executed in said remote log database to record an entry in a log file indicating a possible intrusion in said host. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide an efficiently managing and reporting intrusion, or attempted intrusion, events of a computer network as suggested by Douglas (0004).

Moran and Douglas do not explicitly disclose performing at least one of, the following issuing a command to bring down said one or more network interfaces to isolate said host; issuing a command to an operating system of host to bring said host to a single user state. Trostle, in analogous art, however, discloses performing at least one of, the following issuing a command to bring down said one or more network interfaces to isolate said host; issuing a command to an operating system of host to bring said host to a single user state (figure 4: 78-96; figure 5: 100; column 6: lines 30-42). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Moran and Douglas to include performing at least one of, the following issuing a command to bring down said one or more network interfaces to isolate said host; issuing a command to an operating system of host to bring said host to a single user state. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide a trusted technique for detecting illicit changes to executable programs (e.g., a

"Trojan horse" appended to an executable program by a computer hacker) as suggested by Trostle in (column 3: lines 19-28).

As per claim 19:

Trostle discloses an intrusion detection and isolation method implemented using a monitoring daemon in a host, wherein said digital signature database and said log database are located on a single server or a plurality of servers belonging to a local area network (column 3: lines; 54-65figure 1: 12).

As per claim 20:

Trostle discloses an intrusion detection and isolation method implemented using a monitoring daemon in a host, wherein communications between said host and digital signature database are encrypted (column 5: lines 50-63; figure 5: 88).

As per claim 21:

Trostle discloses an intrusion detection and isolation method implemented using a monitoring daemon in a host, wherein communications between said host and log database are encrypted (column 5: lines 50-63; figure 5: 88).

As per claim 22:

Moran discloses an intrusion detection and isolation method implemented using a monitoring daemon in a host, wherein said digital signature database is an MD5 database (column 31: lines 46-55).

As per claim 23:

Moran discloses an intrusion detection and isolation method implemented using a monitoring daemon in a host, wherein said log database is a SYSLOG database (column 24: lines 47-64).

As per claim 24:

Moran discloses an intrusion detection and isolation method implemented using a monitoring daemon in a host, wherein said data entities are any of the following: system files, configuration files, or directories (column 4: lines 5-35).

Conclusion

5.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

See the notice of reference cited in form PTO-892 for additional prior art.

Contact Information

6.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Techane J. Gergiso whose telephone number is (571) 272-3784 and fax number is (571) 273-3784. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

/T.G/

Art Unit 2137

February 1, 2008